IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 3, March 2015.
www.ijiset.com
ISSN 2348 – 7968

Transmission of text messages using Video Steganography, applying the concept of Randomization.

M.Karthikeyini[1],N.A Divya[2] and A.Nithyasri[3]

[1] Information Technology, Anna University/ Vivekanandha College of Engineering for Women, Tiruchengode, Tamilnadu, India

[2]Information Technology, Anna University/Vivekanandha College of Engineering for Women, Tiruchengode, Tamilnadu, India

[3]Information Technology, Anna University/Vivekanandha College of Engineering for Women, Tiruchengode, Tamilnadu, India

Abstract

The confidential information can be exchanged between two parties with the help of image and video. A video, which is a collection of several image frames could be a better choice for transmitting secret information in a more secured manner. In the proposed paper, a randomized scheme of inserting secret texts in a video is used. To do this, firstly, a video is segmented into photo frames using a matlab code. All the frames are sequentially arranged. Next, secret information to be sent overis embedded randomly in the odd, even, prime, composite memory locations of image pixel values. After this, the frames are cascaded and regenerated back to the video, which looks exactly as the original.

Keywords:Video steganography, Randomized technique, confidential information, photo frames

1. Introduction

The most significant challenge faced by the world of information and communicated technology is the degree of security of the information to be transmitted. To maintain the secrecy of the information, the technique known as “Cryptography”, was adopted, which mainly deals with the encryption and decryption of message. Though this technique has its own advantages, however it suffers from several cryptographic attacks.

Thus considering the necessity of hiding the existence of message along with its valuable contents, another technique known as the “Steganography” came into existence. Steganography can be defined as the technique of hiding information, thus giving no suspicion about the existence of the valuable content to the intruders.

This is an age old technique which gets new dimensions thesedays. Steganography has come up with many forms. Image steganography is the most popular form. Audio and video steganography are the other form of steganography. In this paper, we propose a different approach to the technique of video steganography.

2. Video Steganography

A video can be defined as the collection of image frames in motion. Generally in a running video, when we compare the pixels of any consecutive frames, we would come to a conclusion that only small amount of pixels are modified and rest all remain static. In the proposed work, we would need video to be segmented into frames, in which the valuable secret information will be hidden. Once this is done, the frames are now aligned in order to get back the video.

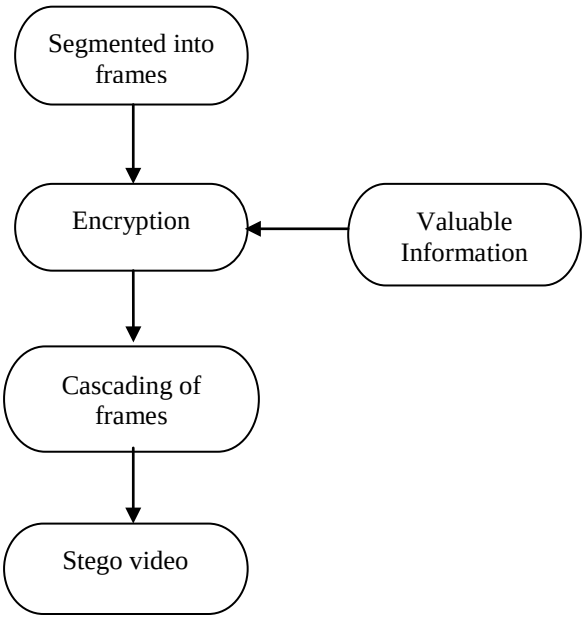


Fig1.1 Video steganography: Encryption

ISSN 2348 – 7968

The authenticated key is generated and exchanged between two parties, who have agreed upon the exchange of confidential information.

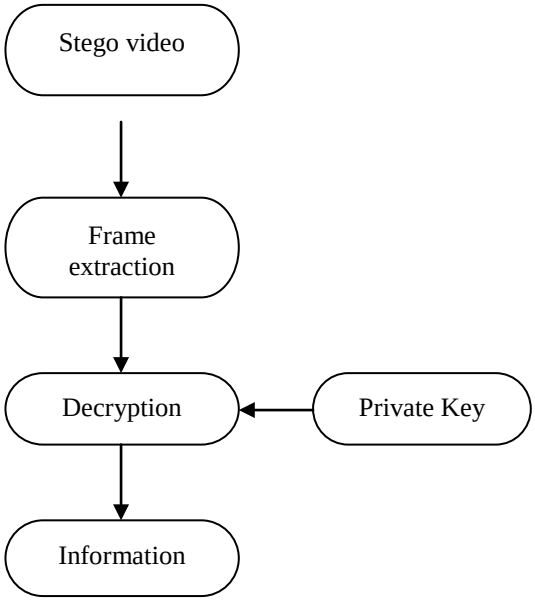


Fig 1.2

Video steganography: Decryption

2.1 Current Techniques in Video Steganography:

2.1.1 Traditional least significant bit substitution:

LSB substitution is the most popular method in steganography due to its ease of application and less perceptual impact. The secret message is converted to a bit stream and each bit of the message is embedded into the LSB of the pixels of the image.

2.1.2 Using Pixel Mapping Technique:

In this technique, a video is distributed into photo frames using mat lab code. Considering a pixel as an 8-bit value and its range from 0-255, two pixels situated at the top left and bottom right corners are modified to insert text in each image. Later the frames are cascaded and reconstructed to the original video.

In these techniques discussed about there are certain disadvantages. In LSB technique, the hidden image can be destroyed by the intruder by changing the LSB of all image pixels. And, in the next technique, more information could not be hidden as only two pixels per frame are modified.

2.2 Proposed Technique for Hiding Valuable Secret Information in Video:

In our proposed technique, the video is distributed into frames using mat lab. And the segmented frames are used for hiding confidential data.

2.2.1 Odd Even Prime Composite Memory Locations:

Embedding secret data in every odd location of the image:

Let the first image of the carrier video be,

30 150**49** **61**70

82 **119** **67**108 92

100 **101**210 **191** 48

64**51** **43** **109** 26

We replace the values with the following message bytes at every odd location we get,

50 48 **101** 24 152

63 **49**94102 83

72125**93**19 55

69 **72**51 96 77

37118**49**21248

Hiding text message in every even memory location:

Let the second image of the cover video be,

4517168109 72

118 1658114 96

32 5113255104

19 29216489

8793 3338 101

ISSN 2348 – 7968

Let the message be

"OWNER"

And the value is

O W N E R

76 83 6712 108

We replace the value with the following message bytes at every even location we get

45**67**68109 72

76165811496

32 **12**13255104

8329216489

87**108**3338 101

Hiding text message in every prime memory location:

Let the third image of the carrier video be,

8558**111**34122

11619 5411133

205 115113 14362

44704199 75

66113 39 23 105

Let the message of "THE" and value is

76 10 24 18 12

We replace the values with the following message byte at every prime location of the image.

8558 **12**34 122

76185411133

10 115113 14362

44 704199 75

24113 39 23105

The same can be extended, even to composite memory location:

Let the message be "APPLE MAC". Considering the same image of the cover video we have,

8558 111**34**122

116 19**54** 11133

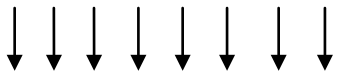
205**115**113 14362

44 70 4199 75

66**113 39**23105

The value is,

A P P L E M A C



72 4 4 22 12 37 72 56

We replace the value with the following message bytes at every composite location we have,

85 4 111 34 122

116 19 3711 133

205 4 113 143 62

72 22 7299 75

66 12 56 23 105

Thus, the randomized approach to video steganography at the odd, even, prime and composite memory locations of the pixel are modified to have an enhanced transmission of secret data over a secured medium.

4. Conclusion

This new approach to Video Steganography possesses the advantages of sending large amount of confidential data to the recipient, as one can embed the data into various pixels of various frames using the concept of randomization as discussed in this paper. Also, since this is a randomization made with video, it can be much secure than could be made with audio or image, as video combines the advantages of both audio and image. Thus, no doubt, this new approach will least arouse suspicion among the intruders and paves a way for high degree of secured transmission of text messages over a medium.

ISSN 2348 – 7968

Acknowledgments

Insert acknowledgment, if any.Sponsor and financial support acknowledgments are also placed here.

References

[1] Metaliya Viral. G, Deepak Kumar Jain, "A Real Time Approach for Secure Transmission of Text using Video Cryptography", IEEE ,2014,Central Electronics Engineering Research Institute, Pilani, Rajasthan.
[2] U.Rizwan, H.Faheem Ahmed, "A new approach to Image Steganography applying Randomization concept",IEEE,2012Islamiah College, Vaniyambadi.
[3] Saurabh Singh, Anurag Jain, "An enhanced text to image encryption using RGB Substitution and AES",IEEE,2013.